Appendix

# 1 SECURITY COOPERATION AUTOMATION

## INTRODUCTION

This appendix provides an overview of some of the more common automation systems used by the security cooperation (SC) community. The overview includes the system description and functionality, as well as the procedures for requesting a user identification and password, if applicable.

## SECURITY ASSISTANCE NETWORK

### Background

In the 1990s, there was heightened interest in developing a more efficient way for overseas Security Cooperation Organizations (SCOs) and geographic combatant commands (GCC) to exchange information with the Department of Defense (DOD) and military department (MILDEP) security assistance management information systems and with individuals at all echelons within the security assistance community. Early in 1990, Defense Security Cooperation Agency (DSCA) formed a special task group to examine security assistance automation among prospective users. One of the objectives was to enhance the opportunity for access by GCC and SCOs, as well as continental United States (CONUS) based security assistance activities, to existing security assistance management information systems and to provide users labor-saving automated data processing (ADP) administrative tools. With this in mind, the director of DSCA established the following goals:

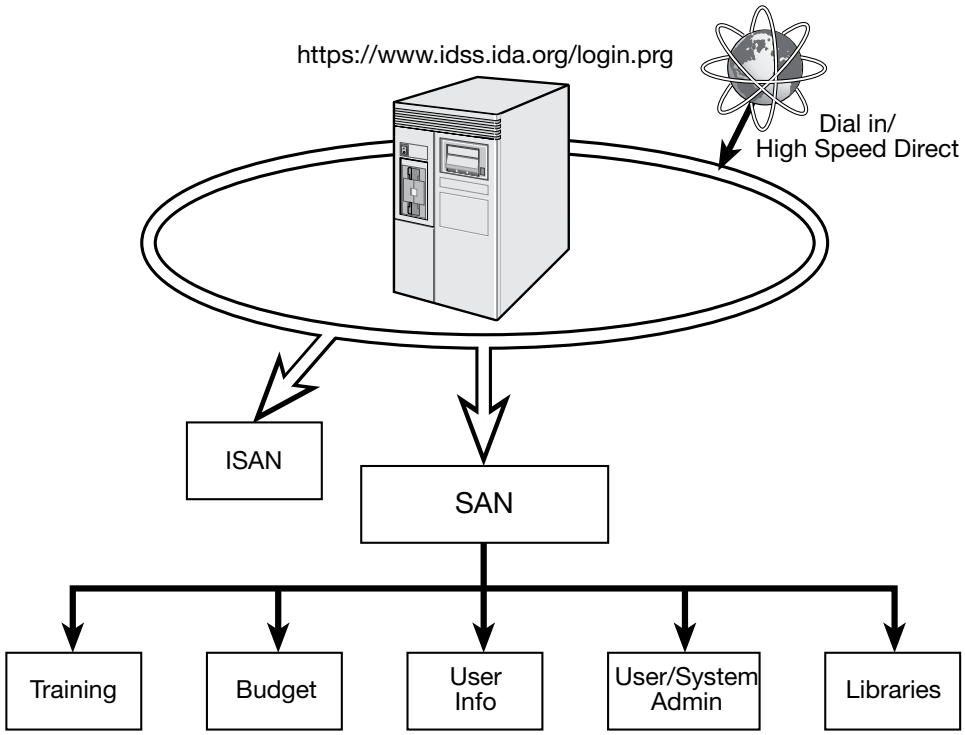
- Tie existing automated systems and users together
- Provide simplified access procedures to a range of automated systems
- Interface automated systems through existing or expanded telecommunications networks, providing automated communication and data exchange support

With the above objectives and goals outlined, the Security Assistance Network (SAN) was initiated, and is currently formalized in DSCA Manual 5105.38-M, *Security Assistance Management Manual* (SAMM), chapter 13. The original telecommunications gateway for the SAN project was the Interoperability Decision Support System (IDSS), operated by the Institute for Defense Analysis (IDA). In the summer of 1996, development began on a web-based SAN. The concept of operations for the SAN web is quite simple. It is a web browser used to connect to the SAN home page via a local Internet service provider.

### System Description

The SAN web contains many useful internal functions. Figure A1-1 shows many of the internal functions available to SAN web users. The SAN web can be accessed at https://www.idss.ida.org/san/login.prg.

**Figure A1-1**
**Security Assistance Network**




## User Database

Students attending the Defense Institute of Security Assistance Management (DISAM) Overseas Course (SCM-O) will automatically be registered as SAN users. Other requests for new SAN accounts can be accomplished by having an existing SAN user, acting as a sponsor, send a request electronically through the system. For detailed information on how to request a SAN account, please see the following web page: https://www.idss.ida.org/sanweb/How%20to%20Request%20a%20SAN%20Acct.doc. Users can locate information about other SAN users by searching the user database. They can search by name, security assistance country code, organization, etc.

## Library

Users can share files with other SAN users by uploading them into one of the libraries. Libraries can also be used to overcome smaller file size limitations of e-mail systems. Information in these libraries must be unclassified.

## Budget

The budget section provides access to the Security Assistance Automated Resource Management Suite (SAARMS) and the Integrated Security Assistance Automated Resource Management Suite (ISAARMS). SAARMS will be discussed later in this appendix. ISAARMS is an electronic interface among the SCOs, the GCC, and the Defense Finance and Accounting Service (DFAS). It is only applicable for Security Assistance Administrative (T-20) funds. Twice a week, T-20 financial information is uploaded from SAARMS to ISAARMS for use by the GCCs and DFAS. GCCs and SCOs can find current and archived data on this site by country or command. DFAS uses this data to update their official accounting records. In return, DFAS produces a file of active financial documents, which is used to reconcile each country's financial records in SAARMS.

### Training

The training section on the SAN provides the user with access to the various international military training databases such as the Training Military Articles and Services List (T-MASL) and the Standardized Training List (STL). SCO users can access this data for their individual countries. MILDEP and GCC users can access multiple countries. Data updates are on a daily basis for all of the military services.

## Training Webs

The Security Assistance Network (SAN) and the Security Cooperation-Training Management System (SC-TMS) are two essential automation systems utilized by the international training community.

Depending on the user's role, International Military Student Office (IMSO) or SCO, different functions will be available to the user as he or she logs into SC-TMS via the SAN.

### SC-TMS for the International Military Student Office

Based on the IMSO role type, various functions are available within SC-TMS for use by IMSOs to manage international military students (IMS) assigned to their schoolhouse. SC-TMS for IMSOs is maintained on and receives its data from the SAN.

SC-TMS for IMSOs provides a means for the IMSO to identify international student quotas assigned to their training activity, receive arrival information on those students and report the student's progress as they advance through the training program. SC-TMS also enables the IMSO to document detailed information about their location and schoolhouse which is available online for the training community.

### SC-TMS for the Security Cooperation Office

SC-TMS for SCOs is maintained on the SAN and receives STL and MASL updates from the Defense Security Assistance Management System (DSAMS). In addition to allowing the SCO to view STL and T-MASL information online, the SC-TMS for SCOs has several other very important features. It is where the SCO enters IMS information and creates Invitational Travel Orders (ITO) for the students. The SCO is also able to look up schoolhouse and IMSO information. The SCO can also maintain SCO POC information within the SC-TMS so that it is available to the training community. SC-TMS is required to be used for submission of student nomination packages for the Combating Terrorism Fellowship Program (CTFP). The SC-TMS is also used by the SCO to submit the Combined Education and Training Program Plan (CETPP).

### International Security Assistance Network Web

The International Security Assistance Network web (I–SANweb) is an Internet tool that provides essentially the same data accessibility to an international user from a host nation that is provided to US SCO users via the SAN. Thus, international users can access the T-MASL data to identify desired courses of instruction. They can see course location information, and can have complete visibility of all country training programs that have been established for their country by viewing the STL. The I–SAN is a read only tool for the international customer. They cannot enter or change any information via the I–SAN. International customers who would like access to the I–SAN should contact their SCO in-country for further guidance. The SCO can then initiate a request for I–SANweb access for the international customer using the main menu of the SAN. The I–SANweb can be accessed at: https://www.idss.ida.org/isan/login.prg.

## Commercial Security Assistance Network

The Commercial Security Assistance Network (C–SAN) is an Internet tool that provides contractors who have an active government contract or other DOD personnel access to the security assistance personnel roster worldwide. Contact DSCA at (703) 601-3733 or rosters@dsca.mil to obtain a user identification and password for this For Official Use Only (FOUO) system. C–SAN can be accessed at https://www. idss.ida.org/csan/login.prg.

## Financial and Logistics Databases

Prior to discussing the financial and logistics databases maintained by DFAS, Army, Navy, and Air Force security assistance agencies, several key points should be noted. First, all access to these databases is read-only, unless special permissions are granted. Although it is recognized that personnel in the SCO and other communities need access to the data, only those personnel responsible for actions have write or change capability. Second, use of the SAN does not require access to or a full understanding of the total database. Thus, SCOs do not see the same screens as the CONUS action offices. Those elements and screens that were deemed necessary were modified and simplified to give the SCO a clear, concise picture of foreign military sales (FMS) case/line/requisition data. Finally, the data viewed is just a snapshot of what is occurring. After viewing, it is considered a historical record because within days, or perhaps hours, the data can change.

### Defense Integrated Financial System

#### *System Description*

The Defense Integrated Financial System (DIFS) managed by Defense Finance and Accounting Service Security Cooperation Accounting (DFAS SCA) in Indianapolis, Indiana, and supported by Defense Security Assistance Development Center (DSADC) in Mechanicsburg, Pennsylvania. DIFS is the integrated DOD financial system for Security Cooperation cases. DIFS is also the interfacing accounting system which links implementing Agency (IA) financial and logistic records with the FMS Billing Statement (DD 645) and supporting financial documents (e.g., FMS Delivery Listing, etc.) issued to purchasing countries and organizations for the articles and/or services that the country has purchased through the Security Cooperation case processes.

#### *Functionality*

Simplified screens have been developed for the US Security Cooperation Organizations (SCOs) providing required data in an easily readable form. For in-country SCOs, data is available for that country only. For the US Combatant Command (CCMD)/Geographic Combatant Commander (GCC) desk officers, data can be made available for all countries of responsibility. For standard DIFS system users the following data is available:

- Country implementing agency (IA) summary totals
- Financial status-country, and financial status-IA for country level data
- LOA detail summary and financial data
- Billing status data
- Payment schedules for LOA
- LOA line level data
- FMS case inventories

- Case controls
- Budget
- Case closure certificate inventory
- Performance/FMS Detail Delivery History Search Reports (FK)
- Cash
- Financial summary totals
- DIFS tables

***Registration***

To register for DIFS access the user must submit a completed DD Form 2875, System Authorization Access Request (SAAR), to DFAS. The basic form is available online: http://www.dtic.mil/whs/directives/forms/index.htm.

DFAS has developed a special continuation sheet that explains what is required in block 27 of the form. To request the continuation sheet and submit the completed form, email DFAS–IN-DIFS-ACCESS-REQUEST@DFAS.MIL or contact the administrator at:

DFAS-JAXDC/IN

8899 E. 56th St.

Indianapolis, IN 46249

Fax: (317) 212-1917 (No DSN)

Tel: (317) 212-0977/7396, DSN 699-0977

**Management Information System for International Logistics**

***System Description***

The Management Information System for International Logistics (MISIL) is the US Navy's logistics and financial tracking system for security assistance. MISIL has standardized screens for SCO use.

***Functionality***

Some of the most useful screens and uses are as follows:

- The case management screen depicts material provided, summary case information, and the name and phone number of the case manager.
- The case/amendment/modification screen provides implementation dates of the latest amendments/modifications and the number of any pending case actions.
- The case line summary screen provides a description and dollar value for every line on an LOA and identifies lines supplying major defense equipment (MDE).
- The case line detail screen provides data such as material supplied, source of supply, disbursements, obligations, for a specific case and line.
- The case financial screen provides financial data for each line of a case as well as case totals.
- The case management history screen shows chronologically the impacts on a case by amendments and modifications.

- The requisition screen provides detailed information on the current supply, shipment, and delivery status of any requisition for a given case.
- The supply discrepancy report (SDR) or report of discrepancy screen gives general and specific information on all SDRs submitted against a case.
- The FMS case listing report area enables the user to generate a complete listing of all cases for a specific country.

In addition to these simplified screens, the SCO also has access to selected MISIL screens, which are used by CONUS FMS case managers.

***Registration***

To obtain access to MISIL, the user must submit a completed DD Form 2875, System Authorization Access Request (SAAR) and forward it to:

NAVSUP WSS-OF

ATTN: P7612 700 Robbins Avenue

Philadelphia PA 19111 Fax: (215) 697-0333

DSN 442-0333 Tel: (215) 697-2774, DSN 442-2774

**Centralized Integrated System for International Logistics**

***System Description***

The Centralized Integrated System for International Logistics (CISIL) is the Army's automated system used to support the management of security assistance programs. CISIL is the central repository for all Army security assistance and provides a series of databases, which offer users of the system information needed to manage their specific program. The system is comprised of modules of data which interact within the system and also interface with other external sites/activities for exchange of information. The SCO menu within CISIL provides access to various levels of information to assist the SCOs in managing the programs under their area of responsibility.

***Functionality***

The CISIL SCO menu provides the user access to logistical and financial information at case, line and requisition levels specific to their programs. It also provides useful case management reports, case history, requisition and supply discrepancy report (SDR) data. One of the areas currently provided under CISIL SCO data is the case requisition review report sometimes referred to as the mini-audit report or case audit report. Although designed for US Army Security Assistance (USASAC) personnel, SCOs may find the open inhibitors option and the case requisition review option very helpful. Much of the same data in CISIL can be viewed in the user-friendly web-based Security Cooperation Information Portal (SCIP).

***Registration***

To obtain access to CISIL, the user must submit a completed DD Form 2875, System Authorization Access Request (SAAR) and a signed CISIL IT Users Agreement and forward them to:

USASAC-S ATTN: Security Manager
54 M Avenue, Suite 1
New Cumberland, PA 17070-5096
(717) 770-4735 DSN: 771-4735 (Fax)
(717) 770-7052/7845; (DSN) 771-7052/7845

### Security Assistance Management Information System

#### *System Description*

The Air Force Security Assistance and Cooperation Directorate (AFSAC) is responsible for administration of the security assistance program within the Air Force Materiel Command (AFMC). Security assistance program activities start with the initial negotiation of agreements for AFMC-managed initial and follow-on support cases, continue with the delivery of logistics support and end with the completion of all financial aspects of the programs for which AFMC is responsible. The Security Assistance Management Information System (SAMIS) is the Air Force's primary logistics information system for security assistance.

#### *Functionality*

The SAMIS maintains and reports comprehensive data on AFMC-managed security assistance programs. This information comes from many different sources; however, most data originates from various Air Force data systems. SAMIS serves as a repository for FMS case information, requisitions, supply status, shipments, and billing information required by AFSAC to effectively manage security assistance programs. SAMIS provides the security assistance community with accurate and timely information. To accomplish this, SAMIS provides online, real-time data updating as well as batch processing functions.

#### *Registration*

The SAMIS is a password protected system. A DD Form 2875, System Authorization Access Request (SAAR) is required for both US government (USG) (including SCOs) and international customers. Access to SAMIS can be requested via the AFSAC web site at https://afsac.wpafb.af.mil, "Apply for AFSAC Online and/or SAMIS Account." Access to SAMIS and AFSAC online is granted based on a person's "need to know." Users are assigned specific permissions and privileges according to their FMS task requirements. Once the SAAR is approved, a user identification and password will be issued. There are four application formats based upon the category of the user:

- USG civilian and military—This category consists of AF, DOD, and other USG employees including those working in overseas locations such as SCOs.
- USG contractor—This category includes contractors employed by USG that need to access FMS data as approved by the command country manager and/or the system administrator.
- CONUS foreign national representatives and support contractors—This group includes foreign representatives and contractors employed directly by the country that work within the continental US (CONUS) such as freight forwarder employees, Foreign Liaison Office (FLO) employees, embassy personnel, and any US citizen employed by a foreign country.
- OCONUS foreign national representatives and support contractors—This category includes individuals listed in above that are located outside of CONUS (OCONUS). It is important to note that this category of user is required to forward their request for access through their embassy in Washington, DC.

## Defense Security Assistance Management System

### System Description

The Defense Security Assistance Management System (DSAMS) is a DOD standard system operating under a modern information technology infrastructure encompassing the migration and reuse of selected features of existing security assistance systems. Incorporating an extensive analysis of the

security assistance business area and its processes, DSAMS provides a set of standardized, improved, streamlined, and optimized services. The major benefits of DSAMS are consolidated data, improved data quality, standard reports to the customer, faster building of cases, and a current implemented view when a case is opened in DSAMS.

**Functionality**

***Case Development Module***

The case development module (CDM) provides functionality from the entry of an initial request through the development of a FMS LOA and changes resulting in a modification or an amendment. The CDM also initializes centralized reference tables and workflow applications that are used in other modules. Enhancements over the past few years include additional functionality to enable electronic countersignature, and support for other security assistance programs such as leases.

***Case Implementation Module***

The case implementation module (CIM) covers the process from receipt of customer acceptance through issuance of implementing directions to the case manager and performing activity.

***Training Module***

The training module (TM) replaced the three MILDEP legacy training management systems, and includes automated interfaces with the SAN and TMS systems. This allows the automated upload of international student data into DSAMS, and automated the invitational travel order (ITO) funding process. DSAMS TM also allows the automated processing of cross-service training requirements across MILDEP channels.

**Registration**

DSAMS is a password protected system for use by USG personnel only. A DD Form 2875, System Authorization Access Request (SAAR) is required for access to DSAMS. Access to DSAMS applications is through the Citrix application only. Applicants for Citrix user accounts must email or fax a completed SAAR to the DSAMS help desk. The e-mail address is saar@dsadc.dsca.mil and the fax is DSN 430-9082. However, the user must have a valid DSAMS account, provided by a MILDEP, before a Citrix account is provided.

Once access is approved, a user identification and password for Citrix will be issued. The issuance of the DSAMS accounts is done through the appropriate MILDEP points of contact. Any additional questions should be directed to:

DSAMS Help Desk

helpdesk@dsadc.dsca.mil

717-605-9200; (DSN) 430-9200

DSAMS does not permit system access by international customers. There is a daily interface from DSAMS to the SCIP which provides FMS customers access to selected DSAMS data.

## Security Cooperation Information Portal (SCIP)

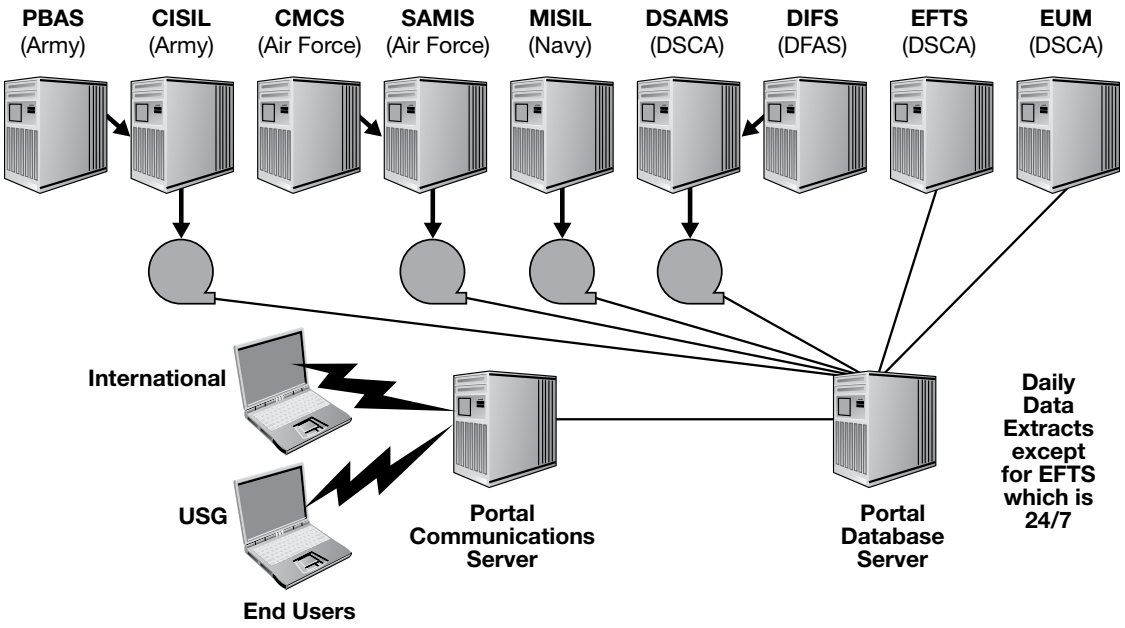
**System Description**

SCIP (https://www.scportal.us/home/) is a secure, controlled, unclassified DOD web-based computer information system that provides authorized users with access to Foreign Military Sales (FMS) and Building Partner Capacity (BPC) programs' case-related data and reports to support management responsibilities for those cases. All USG personnel (including Locally Employed Staff—

LES, and support contractors), and foreign purchasers (including their authorized freight forwarders) who have job responsibilities requiring access (i.e., need to know) to the SCIP system information are eligible to obtain SCIP accounts. DSCA's policy is that "USG personnel and SCOs are encouraged to become familiar with SCIP's full capabilities."

The SCIP data extracts are obtained (automatically for most of the data) from multiple authoritative DOD and US military department (MILDEP) financial and logistics systems (figure A1-2). The majority of data is updated daily via a batch process at 0700 US Eastern Standard Time. Refresh status indicators and information are provided to users in the "Case Info Community" to document the date/time of the last data refresh from those systems. Depending on the data being sought and the user's permissions, having a single SCIP account can save time from having to obtain separate system accounts to access that data from each individual source system. SCIP became operational in 2003 and has been significantly expanded and improved upon over time. SCIP system access is available world-wide from any computer (i.e. does not have to be from a USG or DOD domain) as long as there is adequate internet access, and an active, authorized SCIP user account.

**Figure A1-2**
**SCIP Authoritative Data Sources**



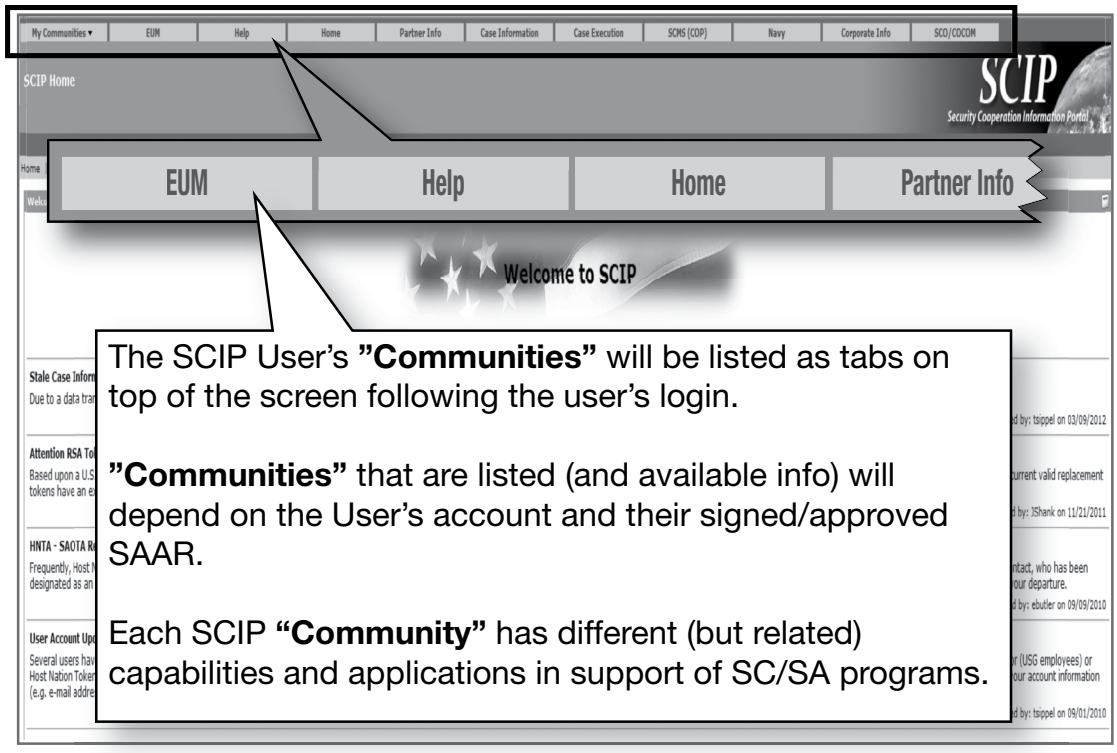

## Functionality

SCIP capabilities, applications, and reports are separated by tabs into different "communities" (see figure A1-3). Some of the SCIP communities are only authorized for USG users. A brief description of each community and the related capabilities and applications follows.

### *Home Community*

This is the first page users see when they successfully logon to SCIP. Like all the SCIP communities, there are announcements to inform the user of all the recently completed and planned changes to that community. Users can use the community navigation bar (Figure A1-3) at the top of the web page to navigate to any of their authorized communities.

**Figure A1-3**
**SCIP Community Menu Bar**




***Case Information Community***

This community provides a query capability to view all FMS and BPC case information for which the user has been authorized to access. SCIP displays region, country, or case data of interest depending upon the user access, application, and filter options that the user chooses. The application is chosen by the user via the "Case Information" menu bar. Each community has a unique menu bar. This unique menu bar is located directly below the "Community" navigation menu bar and available once the desired community is selected. It provides the user with the capability to select their desired community application or report. In the "Case Information" community, some of the applications include real-time metrics (that can be quickly exported to a PowerPoint slide if desired), data inputs (requisitions, supply discrepancy reports [SDRs], freight transactions), Financial Management Reviews (FMRs), Ad Hoc reports, and a Case Status filter to enable the user to quickly find cases of interest. For all cases that the user is authorized to see, the user is presented with a "Pyramid of Choices" (figure A1-4) for all the case's Letter of Offer and Acceptance (LOA) documents (Basic, Amendments, Modifications). Selecting any one of these pyramid levels will provide the user with specific case details (e.g., what is the LOA Anticipated Offer Date, when is the requisition material expected to be shipped, are there any unprogrammed case funds remaining, etc.) pertaining to that level. A summary report of all or a portion of that case data can be exported to a Microsoft Excel file.

***Case Execution Community***

This community provides links to several tri-service applications, including the Enhanced Freight Tracking System (EFTS), EMALL, Asset Visibility (AV), and the recently added WebRoR (formerly a Navy-only application that automates the repair of repairable process). EFTS is a secure, web-based application that serves as a consolidated source for SC material in-transit information. EFTS does not replace existing shipment systems, but rather, it provides a clearing house of all available shipment

information in a single supplemental tracking system to provide additional visibility of equipment and material shipments. EFTS receives data from Defense Logistics Agency (DLA), contractors, depots, Defense Transportation System, carriers, freight forwarders, consolidation points, and ports of embarkation and debarkation. This allows EFTS to provide visibility of the SC material distribution pipeline for all classes of supply and modes of transportation either outbound from the US to the purchaser's country or materiel returning to the US or US facilities overseas.

**Figure A1-4**
**Case Status Menu Options—A "Pyramid of Choices"**


***EUM (End-Use Monitoring) Community***

This community provides authorized users with specific information, reports, and capabilities applicable to the DOD EUM program. The EUM applications within SCIP provide inventory reports that will help inspectors plan for upcoming inventories and isolate items that are considered "delinquent."

***Partner Info Community***

This community is an information-sharing type of community vice a business process or business application community. It includes (among other items) documents, presentations, and files related to the Foreign Procurement Group (FPG), and International Customer User Group (ICUG).

***National Geospatial-Intelligence Agency (NGA) Community***

This community allows authorized SCIP users to access, review, and download navigation charts (e.g., aeronautical en route and approach charts, terminal procedures, etc. for international navigation and flight safety).

***Security Cooperation Management Suite Community SCMS (COP)***

Access to this community is authorized only for USG personnel to support case management responsibilities for Building Partner Capacity (BPC) and Foreign Military Sales (FMS) cases. SCMS resides within the SCIP and is a joint-service, web-based capability that provides a common operating picture of the SC process. It shows the FMS, FMF, and BPC cases for a country in pie chart and

Excel formats. SCMS has joint worldwide US military and civilian users, which increases joint communication, resulting in enhanced decision making. SCMS provides USG personnel with key information used to track high-priority FMS and BPC programs and is especially useful during the oversight process for expiring funds on cases that are funded via US appropriated sources. SCMS allows data input and customization through its multiple reports, showing information by appropriation and program, which allows for vital information sharing among multiple program participants. Although initially conceived to support the war effort in Iraq, the utility of SCMS was recognized by additional communities throughout the DOD. SCMS has been expanded for use with all the BPC programs. It benefits US decision makers when planning how to best build partner nation capacity.

***Corporate Info Community***

This community provides information to USG personnel regarding the Security Cooperation Business Forum (SCBF) and Performance Measurement Senior Working Group (PMSWG) meeting, Lean Six Sigma/Continuous Process Improvement, organizational charts, Lessons Learned—Best Practices, etc.

***SCO/COCOM Community***

Access to this community is authorized only for USG personnel and provides an information sharing (e.g. General Information, Lessons Learned & Best Practices, etc.) for the USG SCO and GCC personnel.

***Navy Community***

This community provides numerous capabilities (e.g., Case Execution Performance Tool– CEPT, Case Reviews, Information Warehouse, Supply Discrepancy Reports, etc.) pertaining to US Navy-managed cases. Case and line financial commitments, obligations, and expenditure details are also provided for those cases.

***Air Force Community***

This community provides information on the T-6 Texan II and a link to AFSAC and SAF/IA.

***Help Community***

The help desk was developed to provide all SCIP users a common location and interface for submitting and reading SCIP help desk requests. Having the help desk embedded within SCIP provides users with more security and privacy and prevents unauthorized viewing of requests. There are also numerous online help guides (Help Desk User Guide, Case Information User Guide, SCIP Help Descriptions, Corporate Info User Guide, International Customer Token Access Guide, Logon Guide, SCIP Acronyms, SCIP Background, Token Administrators Guide, US Government (USG)/SCO Token Access Guide, and the Partner Info User Guide) posted to assist SCIP users with understanding how to fully use the numerous SCIP capabilities. In addition to the guides and reference documents listed above, there are also other Community specific guides that are posted on SCIP that can be accessed via the Help links on the applicable community navigation menu.

**Obtaining a SCIP Account**

The online SCIP registration form for both US and international users can be found by accessing the SCIP web site (https://www.scportal.us/home/) and clicking the "REGISTRATION INFO" link on that page. All USG SCO and GCC students that attend the DISAM Security Cooperation Management Overseas (SCM-O) course are registered for their individual SCIP accounts while in class per the DSCA Policy Memo 11-58 (*Policy Update Regarding Security Cooperation Information Portal (SCIP) Account Access for Security Cooperation Officers (SCOs)*). For all other SCIP account

applicants, follow the instructions in the SCIP "REGISTRATION INFO" introduction to submit the registration for processing by the SCIP Program Office/Defense Security Assistance Development Center (DSADC). International (i.e., non USG) SCIP applicants must be issued a secure SCIP token by their country's Host Nation Token Administrator (HNTA) prior to completing the registration form. DSCA Policy Memoranda 03-11 (*Enrollment Process for the SCIP*), and 05-17 (*SCIP Electronic Token Issuance and Replacement Processes*) are the policy references for details regarding issuance and management of SCIP tokens. The SCIP International Customer Token Access Guide (posted on the SCIP "REGISTRATION INFO" web page), provides further details on SCIP token operations and processes. Additional SCIP DSCA policy memoranda are posted on the DSCA web site. For additional SCIP assistance, users (and prospective users) can contact the SCIP Help Desk at dsca.sciphelp@mail.mil or via phone at (717) 605-9200.

**Accessing the Security Cooperation Information Portal (SCIP) Web Site**

To access the SCIP system once a user has obtained a SCIP account, type https://www.scportal.us/home/ in the Internet browser address line and click the "SCIP Logon" link on top of that page. Both Internet Explorer (IE) and Mozilla Firefox can be used to access SCIP, though SCIP functionality appears to work best on IE. The browser advanced security settings and DOD root certificates need to be correct to gain access. Also, ensure pop-ups are allowed. Contact the SCIP Help Desk regarding SCIP log-on issues.

If logging into SCIP with a USG Common Access Card (CAC) certificate, (which is the usual means for USG DOD users to log-on to SCIP if the account has been CAC enabled), select the non-e-mail certificate. Logging into the SCIP system with a token will be via the subsequent SCIP login screens requiring entry of the SCIP user ID and passcode.

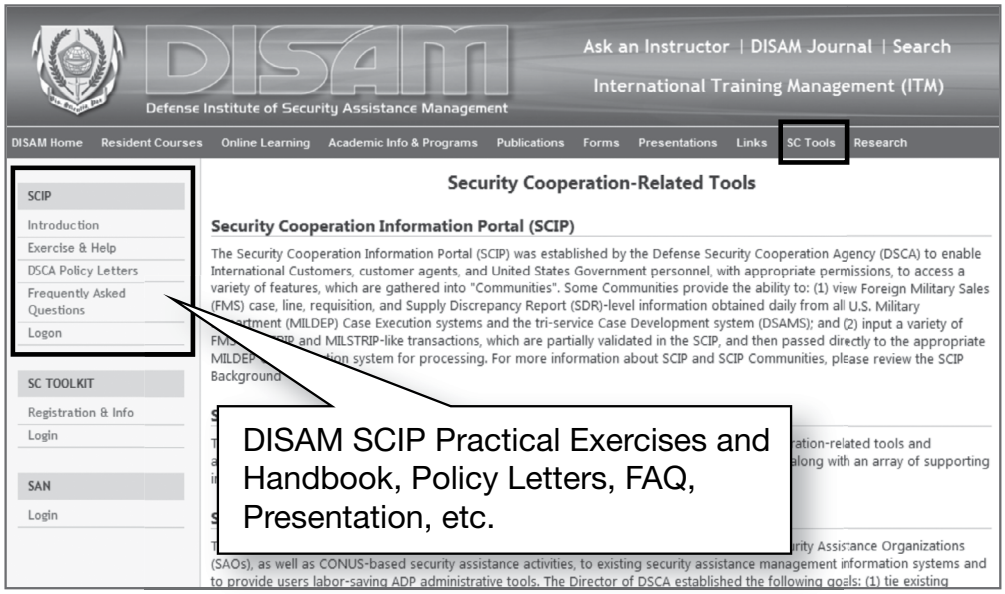
To keep the SCIP account active, users need to periodically log-on. The current policy is to suspend user accounts for non-use at 30 days, requiring you to contact the SCIP Help Desk at dsca.sciphelp@mail.mil for account reactivation. At 180 days of non-use, your account will be terminated, requiring you to complete and submit a new registration form to obtain a new SCIP account.

***SCIP Training***

DISAM provides SCIP basic through advanced topic training in the majority of the DISAM-offered classes. The DISAM SCIP classroom training, which includes in-residence and Mobile Education Teams—METs, has expanded significantly in the past few years due to the increasing importance of SCIP to the SC users. Electronic copies of current DISAM SCIP presentations are posted on the SCIP Corporate Info Community and are accessible via the "Training>DISAM Presentations>SCIP" links to authorized USG users. The DISAM SCIP training maximizes the online demonstration of the system capabilities by the instructors and the 'hands-on' practical exercises by the students.

Additional SCIP information and training may be accessed on the DISAM home page (http://www.disam.dsca.mil/) via the "SC Tools" link on that page. These DISAM SCIP training resources (figure A1-5) include an overview presentation, a SCIP exercise handbook, DSCA SCIP policy letters, SCIP frequently asked questions (FAQs), and a link to access the SCIP system. The SCIP handbook is a familiarization tool and training guide for SCIP users to better understand the capabilities of the SCIP system. It is intended for both initial system instruction, and also to provide users with future reference handbook when utilizing the SCIP system. All the exercise questions (Process, Logistics, Financial, Miscellaneous Advanced) in the handbook are based on information provided in the DISAM class lessons and can be completed even without a SCIP account using the case examples in the handbook. A basic understanding of the FMS process, logistics, and finance subjects is needed to understand and interpret the materials and complete the exercises in the SCIP exercise handbook. Other DISAM SCIP training includes online training module 'vignettes', which students can access and complete via the DISAM web page under "Online Learning."

**Figure A1-5**
**SCIP on DISAM Web Page**




## Additional Software Packages

### Security Assistance Automated Resource Management Suite

#### *System Description*

The Security Assistance Automated Resource Management Suite (SAARMS) is a group of one stand-alone and two web-based software applications used by SCOs and GCCs to manage their security assistance funded resources. The SAARMS applications are Budget Preparation, Budget Execution, and Property.

#### *Functionality*

Budget Preparation—This program standardizes the budget preparation process in a web-based format. It uses relevant historical data from previous budget submissions and periods of financial execution and generates the required budget submission reports that SCOs and GCCs are required to submit to DSCA during the budget submission cycle.

Budget Execution—This program is a web-based funds management feeder system that automates the record keeping of the SCO budget management functions. SAARMS feeds into the official DFAS BQ accounting system by conducting twice-weekly electronic transfers of data via the SAN.

Property—This program is a stand-alone application that is used for property book management, to include accounting for property and tracking property acquisition, use, and disposition.

### International Training Management Web Site

The International Training Management (ITM) web site is an informational web site intended for all US and foreign international training managers. It provides a full range of international training management information, including references, policy and procedural messages, articles, lessons, exercises, FAQ sheets, links, and specific functional information.

The ITM web site is available to anyone at http://www.disam.dsca.mil/itm/ and does not require the use of a password.

**DOD Acquisition Portal**

***System Description***

The DOD Acquisition Portal is designed to be a single point of access to DOD acquisition related resources and information. This web-based system easily links users to the myriad of acquisition source documents, references, and other related information. The acquisition portal replaces its two predecessors, the Acquisition Knowledge Sharing System (AKSS) and the previous Defense Acquisition Deskbook (DAD) system.

***Functionality***

Acquisition Process—Covers the three primary acquisition processes of the Joint Capabilities Integration and Development System (JCIDS), the Defense Acquisition System (DAS), and the Planning, Programming, Budgeting and Execution (PPBE) system. This includes links to DOD and MILDEP policies, guidance, tools and other resources.

Workforce—Provides information on acquisition career management, the DOD human capital initiative, career planning, leadership training, and relevant professional organizations.

Policy—Serves as an encyclopedic source of acquisition policy that follows a hierarchy of policy issuance that can also be filtered by organization, career field and special topics.

Communities of Practice—Offers links to the various acquisition communities of practice and special interest areas.

Training and Continuous Learning—Outlines various training resources and continuous learning opportunities applicable to DOD acquisition professionals.

Industry—Functions as a one-stop source for information and links about industry partner support and participation in defense acquisition.

Workforce Support—The acquisition portal also provides a link to the DAU's "Ask a Professor" (AAP) program. AAP serves as a vehicle for practitioners within the DOD workforce to submit acquisition related questions that are routed to the appropriate subject matter expert for a response. AAP contains a user accessible Frequently Asked Question (FAQ) database that can be searched by key word or by category. FMS related questions are contained within the "International Foreign Military Sales" sub-category within the overall "Contracting" category.

***Registration***

The acquisition portal is hosted by the Defense Acquisition University (DAU) on behalf of the DOD acquisition community. You can access the acquisition portal at https://dap.dau.mil/Pages/Default.aspx. The portal structure consists of a home page with general acquisition information and links.

## SUMMARY

Security cooperation personnel have access to numerous automated systems, some that have been in existence since as early as 1976. Access has transformed from direct links for a few specific users to worldwide access via the Internet. Newer systems such as the SAN and SCIP have been specifically designed with the needs of the end-user in mind. SC users in the far-flung corners of the globe are freed from the constraints of time zone differences and slow mail delivery by virtue

of Internet connectivity and interaction. Use of these systems has greatly enhanced communication between the SCO, GCCs, and CONUS-based logistics and training activities such as the MILDEPs and IMSOs and the international customers. The impact the increased access to the systems discussed in this annex has been profoundly beneficial, not only to security cooperation activities, but ultimately to the international customer as well.

## References


DSCA Manual 5105.38-M. *Security Assistance Management Manual* (SAMM). Chap. 13, sections C13.6.3.2.2, C13.6.3.2.3 http://www.dsca.osd.mil/samm/.

DSCA Policy 03-11. *Enrollment for the Security Cooperation Information Portal*. June 25, 2003. http://www.dsca.mil/samm/PolicyMemos/2003/DSCA%2003-11.htm

DSCA Policy 5-17. *Security Cooperation Information Portal (SCIP) Electronic Token Issuance and Replacement Processes*. June 24, 2005. http://www.dsca.mil/samm/PolicyMemos/2005/DSCA%2005-17.htm

DSCA Policy 11-08. S*ecurity Cooperation Information Portal (SCIP) Background Document*. February 10, 2011. http://www.dsca.mil/samm/PolicyMemos/2011/DSCA%2011-08.htm.

DSCA Policy 11-58. *Policy Update Regarding Security Cooperation Information Portal (SCIP) Account Access for Security Cooperation Officers (SCOs)*. November 15, 2011. http://www.dsca.mil/samm/PolicyMemos/2011/DSCA%2011-58.htmhttp://www.dsca.mil/samm/PolicyMemos/2003/DSCA%2003-11.htm

*SCIP International Customer Token Access Guide*. October 2012. https://www.scportal.us/home/docs/IntlCustAccessGuide.pdf